REMARKS

In the first Office Action, the Examiner rejected claims 1-95 under the judicially created doctrine of obviousness-type double patenting based on a number of commonly owned pending applications and issued patents. The Examiner rejected claims 1-95 under 35 USC §102(b) as being anticipated by Ananda (US 5,495,411).

While Applicant does not agree with the double patenting rejection, due to the number of pending claims and the number of references alleged to render the claims unpatentable, Applicant submits herewith a terminal disclaimer to obviate the double patenting rejection.

Applicant respectfully disagrees with the Examiner's rejection under 35 USC §102(b) based on Ananda (US5,495,411) and traverses the rejection for the reasons described in detail below.

Reconsideration and re-examination of the application considering the following remarks is respectfully requested.

Double Patenting

The Examiner rejected claims 1-95 for obviousness-type double patenting. While Applicant does not agree with the Examiner's position, Applicant submits herewith a Terminal Disclaimer to obviate the Examiner's rejection and advance the prosecution of this case.

Rejection Under 35 USC §102(b)

The Examiner rejected claims 1-95 as being anticipated by Ananda (US 5,495,411). Applicant respectfully disagrees and traverses the Examiner's rejection.

A rejection for anticipation requires that each and every element of Applicant's claims be disclosed explicitly or inherently in a single reference. As described in greater detail below, Applicant's claims include a number of features that are not disclosed in Ananda '411, and Applicant respectfully requests the Examiner to reconsider and withdraw the rejection.

Summary of Ananda '411

The following summary includes features disclosed by Ananda that use similar terminology differently from Applicant, and are distinguishable from Applicant's claimed invention as described with respect to particular claims in the section following.

The '411 reference cited by the Examiner is directed to a software rental system using continuous password verification. The system allows a remote user computer system 150 to use application software downloaded from a central rental facility 180 only while the remote user computer system 150 is electronically connected to the central rental facility. This is accomplished by attaching additional header software 320 (Fig. 3) to the application software 310. Header software 320 includes a rental security manager 321 having modules for authorization verification 321A, execution termination 321B, encryption/decryption 321C, message processor 321D, password generation 321E, and password validation 321F.

During operation, a user provides a user identification password to access the central rental facility 122 (and remote computer 180), which compares the user password to user identification information in registration database 212 to determine if the user password is authorized (Col. 8, ll. 7-38). The user then selects an application program from the rental application database 214. In response, multiuser controller 222 transfers the selected application software 310 and header software 320 through modem 126 to the remote user computer system 150 (Col. 8, ll. 54-64). Central rental facility 122 records the processor clock time of the transfer and an application ID in a file for subsequent use in generating passwords, as well as sending an encrypted message with this information to the user computer system 150.

The rental security module 321 in the header software 320 on the user computer uses 1) the difference between the transfer time from the Central Rental Facility computer 180 and the local processor clock time, and 2) the user password entered to gain access to the Central Rental Facility, as input to a pseudorandom number generator to generate an authorization verification password that is associated with the software by an application ID number. The user computer clock time, user ID password, and authorization verification password are sent to the Central Rental Facility, which also uses 1) the difference between the stored transfer time and the current clock time of the user computer, and 2) the user ID password as input to a pseudorandom number generator that generates an authorization verification password, which is sent back to the Rental Security Module on the user computer. The authorization verification passwords are compared by the Rental Security Module 321 to determine if the SW is authorized. This process is repeated every 100 ms to ensure a continuous connection between the Central Rental Facility and the local user computer. If the authorization verification password comparison

fails 3 times, execution of the application software program on the local user computer is terminated by termination module 321B (Col. 15, ll. 7-63).

Distinguishing Features of Applicant's Independent Claims

Applicant's claimed invention as claimed in independent claims 1, 40, 48, and 81 is a method for securing software to reduce unauthorized use. As claimed in independent claim 1, Applicant's invention requires a primary user device (such as a desktop or laptop computer, for example) and a secondary device (such as a digital content player, for example). Ananda '411 does not disclose any such secondary device.

As claimed in claim 40, Applicant's invention requires determining whether an authorized representative entity is available, and using that entity or installing an authorized representative entity if one is not currently available. Ananda '411 does not make any determination of whether an authorized representative entity is available, or whether or not to install an authorized representative entity.

As claimed in claim 81, Applicant's invention requires obtaining registration information associated with at least one portable user device and transferring the software to a user computer. Ananda '411 does not disclose any portable user devices as claimed by Applicant.

Various dependent claims (i.e. 8, 9, 13, 15, etc.) include a local authorized representative entity installed on or in the primary and/or secondary user device to control access to the software. The user devices may include one or more primary devices, such as a computer, in addition to one or more secondary devices, such as a digital content player, for example (Para. 17). The method may also optionally use a remote authorized representative entity in combination with the authorized representative entity installed on or in the user device, or if a local authorized representative entity is inoperable or unavailable.

With respect to claim 1, Ananda does not disclose obtaining registration information corresponding to at least one authorized secondary device as disclosed and claimed by Applicant. The only registration information disclosed in Ananda is related to identification of the user, not an authorized secondary device. (Col. 8, ll. 7-22). Computer 150 disclosed by Ananda is a primary user device and not a secondary device as claimed. Note that claim 1 requires that the registration information correspond to an authorized secondary device and transferring the software to a primary user device. The method also requires determining whether a

current secondary device (which may be the authorized secondary device identified in the previous step or another secondary device) is authorized. Ananda simply does not disclose anything that can be properly interpreted as anticipating these steps of Applicant's claim.

With respect to claim 2 Ananda discloses that the software is an application program, but does not disclose that the data represents music, video, game, movie, graphics, watermarked works, a magazine, or a book as disclosed and claimed by Applicant. The lines referred to by the Examiner (col. 1, ll. 17-19) describe prior art databases where information such as news, weather, sports, etc. is not protected once it is downloaded, i.e. the user "transfers information to the user's PC, and [it] is further useable without being connected to the database of the centralized computer system." (Col. 1, ll. 21-25).

As per claim 3, the lines cited by the Examiner (col. 3, ll. 11-15, 21-28) describe the process of the user providing a password to the database computer of the remotely located Central Rental Facility. If the Examiner is interpreting this as the registration information, then the step of transferring the software is not performed before obtaining registration information, generating an authentication code, and associating the authentication code as claimed by Applicant.

Applicant's claim 8 states that obtaining registration information is performed by an authorized representative entity installed on or in the primary user device, not a remotely located authorized representative entity. As described above, Ananda discloses that registration information, such as a password entered by a user, is provided to the remotely located authorized representative entity, not a local representative entity installed on or in the user device. Applicant's claimed method provides the advantage of keeping registration information associated with one or more user devices local as described in Para. 10, for example.

As per claim 9, Ananda does not disclose any secondary user device, and therefore does not disclose an authorized representative entity installed on or in a current secondary user device as disclosed and claimed by Applicant..

As per claim 10, Ananda does not disclose an authorized representative entity installed on or in the primary device in addition to an authorized representative entity installed on or in the current secondary user device as claimed by Applicant.

As per claim 11, Ananda does not disclose a secondary user device and therefore does not disclose that the authorized representative entity is remotely located relative to the primary and secondary devices as claimed.

As per claim 12, Applicant's invention requires obtaining registration information corresponding to the primary user device and at least one secondary user device. Ananda does not disclose obtaining registration information associated with the user computer, only with the user. Ananda does not disclose any type of secondary device and therefore does not disclose obtaining registration information associated with the secondary device as disclosed and claimed by Applicant.

With respect to claims 13-14, Ananda does not disclose installing an authorized representative entity on or in at least one of the primary and secondary user devices. As described above, the only authorized representative entity disclosed by Ananda is located at the central rental facility. In addition, Ananda does not disclose any secondary devices.

As per claim 15, Ananda does not disclose any secondary device. Furthermore, Ananda transfers the software to the user computer without regard to whether the user computer is authorized or not authorized. Ananda requires the software transfer time to generate the authorization verification password. While Ananda may terminate the application software if the authorization verification passwords do not match, there is no disclosure of preventing transfer of the software to an unauthorized device as disclosed and claimed by Applicant.

As per claim 16, there is no disclosure in Ananda of modifying the software in any respect if the user device is unauthorized. Ananda only discloses terminating the application program if the authorization verification passwords do not match. As such, there is no disclosure of generating reduced quality software and transferring the reduced quality software to the current secondary device as disclosed and claimed by Applicant.

As per claim 17, the Examiner cites Col. 10, ll 4-15 as not only disclosing a secondary device, but that the secondary device is a digital audio player as disclosed and claimed by Applicant. However, the passage relied upon is directed to one function of the header software 320. There is simply no disclosure of a secondary device, or that the secondary device is a digital audio player as claimed.

As per claim 18, Ananda does not disclose any secondary devices, and therefore does not disclose that controlling access to the software is performed by the secondary device as claimed.

As per claim 20, there is no disclosure in Ananda of a secondary device and no disclosure of transferring software to an authorized secondary device with the authentication code. As described above, Ananda can not transfer the

authentication code with the software because the authentication code disclosed by Ananda requires the software transfer time. As such, even if Ananda disclosed a secondary device, Ananda does not transfer the authentication code with the software as claimed.

As per claim 21, Ananda makes no determination as to the functionality of the authorized representative entity as claimed by Applicant. Furthermore, there is no disclosure of determining if there is an operable authorized representative entity on a current secondary device because Ananda does not disclose any secondary devices, and the only authorized representative entity is remotely located at the central rental facility.

As per claim 22, Ananda does not disclose any secondary device and does not disclose determining whether an authorized representative entity is available. As such, Ananda does not disclose installing the authorized representative entity on the secondary device if an operable authorized representative entity is not detected. To the contrary, Ananda transfers the software to the user computer without regard to whether the software has previously been transferred (See Col 18, ll. 50+).

As per claim 23, Ananda transfers the software to the user computer whether or not the computer is authorized. The authorization verification passwords that are subsequently generated determine whether to terminate execution of the application program and use the transfer time from the central rental facility.

As per claim 24, Ananda does not disclose identification of any user device, only identification of the user. The only prompt disclosed by Ananda is when the user is prompted to enter a password to access the central rental facility. There is no disclosure of prompting the user to identify any user device, and no disclosure of prompting the user to identify a secondary device as claimed.

As per claim 25, the Examiner cites the same passage used in rejecting claim 24. However, claim 25 requires that the registration information is automatically obtained from the secondary device. Ananda does not disclose any secondary device and therefore does not disclose obtaining registration automatically from a secondary device as claimed.

As per claim 26, Ananda does not disclose any secondary device, nor an authorized representative entity installed on a primary device, and therefore does not disclose determining whether a current secondary device is authorized using an authorized representative entity installed on a primary user device connected to the secondary device as claimed.

As per claim 27, there is no disclosure of wireless communication between a primary and secondary device in Ananda.

As per claim 28, there is no disclosure of any secondary devices in Ananda. As such, there is no disclosure of the secondary device being a personal digital assistant as claimed.

As per claim 29, Ananda transfers the software to the user computer before determining whether the user computer is authorized. This is required because the authorization verification password in Ananda requires the transfer time from the central rental facility. As such, there is no disclosure of preventing transfer of at least a portion of the software to the current secondary device as claimed.

As per claim 30, there is no disclosure of a secondary user device and therefore no disclosure of preventing a secondary user device from utilizing the software as claimed.

As per claim 31, there is no explicit disclosure of different file types in Ananda. The only suggestion of a file type is relative to the application software, which is presumably an executable or .exe file type. However, there is certainly no disclosure of a second file type or controlling access to the software by a secondary device by providing a second file type as claimed by Applicant.

As per claim 32, there is no disclosure in Ananda of a secondary device, and clearly no disclosure of having the steps of obtaining, generating, and associated performed by the primary user device and the steps of determining and controlling performed by the current secondary device as claimed.

As per claims 34-36, there is no disclosure in Ananda of an identifier that triggers authentication, of disabling the means for generating the authentication code, of including the software on a computer readable storage medium as claimed by Applicant.

As per claims 37-38, Ananda discloses an authorization verification password that is based on the user password, the transfer time of the software, and the clock time of the local processor. There is no disclosure of an authentication code that at least partially corresponds to a particular type of secondary device, or a secondary device manufacturer. As previously stated, Ananda does not disclose any secondary devices and certainly not an authentication code corresponding to a particular type of secondary device, or a secondary device manufacturer as claimed.

As per claim 40, Ananda does not intercept a request to access the software or make any type of determination with respect to whether an authorized

representative entity is available. The steps performed for authentication as disclosed by Ananda are performed without regard to whether an authorized representative entity is available. Ananda discloses transferring the software with the rental security manager without regard to whether the software was previously transferred or installed on the user computer.

As per claim 42, there is no disclosure of intercepting a request to transfer software from a primary device to a secondary device. Ananda does not disclose any secondary devices.

As per claim 43, Ananda does not disclose intercepting a request to utilize the software as claimed. As described previously, during execution of the application software, Ananda compares the authorization verification passwords to determine whether the user device is authorized and terminates the application program if not authorized.

As per claim 44, Ananda does not disclose any secondary device, or determining whether an authorized representative entity is installed on or in a secondary device as claimed. Rather, Ananda transfers the software to the user computer whether or not it has been previously transferred or otherwise installed on the user computer.

As per claim 45, Ananda does not transfer software to a secondary device. Ananda transfers the software to the primary device before any determination of whether the device is authorized because Ananda uses the transfer time to generate the authorization verification passwords. As such, Ananda does not disclose transferring the software to a secondary device if the device is determined to be authorized as claimed.

As per claim 46, Ananda does not disclose a secondary device and therefore does not disclose a primary device that determines whether a secondary device is authorized.

As per claim 47, Ananda does not disclose a secondary device in addition to the primary device and authorized representative entity. As such, Ananda does not disclose using a remotely located authorized representative entity to determine whether a secondary device is authorized.

As per claim 48, Ananda does not associate an identifier with the software and detect the identifier to request authentication. Rather, the steps of Ananda are performed without regard to the presence or absence of any identifier. Ananda does not disclose any secondary device, or obtaining registration information associated

with at least one secondary device. The only registration information disclosed in Ananda is the user password that is associated with the user and not the user device. Likewise, there is no disclosure of controlling access to the software by a secondary device as claimed by Applicant.

As per claim 49, the only prompting of the user for information disclosed in Ananda is during the initial access to the central rental facility where the user is prompted to enter a password. The password identifies the user (if it has not been copied or otherwise compromised) and not a particular user device. Certainly, there is no disclosure of prompting the user to identify a secondary device as claimed.

As per claim 51, Ananda does not disclose registration information associated with any user device. As such, there is no disclosure of automatically obtaining hardware information from a secondary device as claimed by Applicant.

As per claims 52-53, there is no disclosure in Ananda of the authentication code at least partially corresponding to a secondary device manufacture or a specific type of secondary device. The authorization verification password disclosed by Ananda is based on the user identification password, the transfer time that the software is transferred from the central rental facility, and the local processor clock time of the user computer.

As per claim 54, Ananda specifically states that the authorization verification password is NOT communicated between the central rental facility and the user computer. In addition, the authorization verification password requires the transfer time of the software and therefore can NOT be embedded within the software as claimed by Applicant.

As per claim 55, Ananda does not disclose modifying the software based on the authentication code as claimed by Applicant.

As per claim 56, Ananda transfers the software to the user computer prior to determining whether the user computer is authorized. Because the authorization verification password requires the transfer time, Ananda can not prevent the software from being transferred to an unauthorized device as claimed. Furthermore, there is no disclosure in Ananda of secondary devices, such that Ananda does not disclose preventing the software from being transferred to an unauthorized secondary device as claimed.

As per claim 57, Ananda does not disclose any secondary devices and therefore does not disclose preventing secondary devices from utilizing the software as disclosed and claimed by Applicant.

As per claim 58, the authorization verification password of Ananda requires the transfer time of the software. As such, Ananda does not disclose generating an authentication code PRIOR to distribution of the software as claimed by Applicant.

As per claim 59, Ananda discloses transferring the software over a telephone network. There is no disclosure of software distribution on a computer readable storage medium as claimed.

As per claim 61, Ananda discloses a remotely located authorized representative entity that must be in continuous communication with the user computer. There is no disclosure of installing the authorized representative entity on the primary user device as claimed. Similarly, because Ananda does not disclose any secondary device, there is no disclosure of installing an authorized representative entity on the secondary device as claimed.

As per claim 62, there is no disclosure in Ananda of installing the authorized representative entity from a computer readable storage medium as claimed.

As per claim 63, there is no disclosure in Ananda of installing the authorized representative entity on a user device and therefore no disclosure of installing the authorized representative entity from a network.

As per claim 64, Ananda transfers the software to the user computer prior to any determination of whether the computer is authorized. As such, Ananda does not disclose preventing the software from being transferred to any device, and does not disclose transferring the software to an unauthorized secondary device as claimed.

As per claim 65, Ananda discloses a user password provided by the user during initial access to the central rental facility. However, there is no disclosure of automatically obtaining registration information associated with a primary user device and at least one secondary user device.

As per claim 66, Ananda does not disclose restricting access to the software by a secondary device and does not disclose automatically identifying a secondary device. As such, Ananda can not disclose restricting access to the software if registration information can not be automatically obtained as claimed by Applicant.

As per claim 67, Ananda discloses terminating access to the application software if the authorization verification passwords do not match. There is no disclosure of providing limited access to the software by a secondary device if the device can not be automatically identified by an authorized representative entity installed on the primary device as claimed.

As per claim 68, Ananda does not explicitly disclose any file types. The application software is presumably an executable file, such as an ".exe" file type. However, there is no disclosure of a specific file type for use with secondary devices (especially because Ananda does not disclose any secondary devices).

As per claim 69-71, Ananda does not disclose any secondary devices and certainly does not disclose a portable device such as a digital audio player or cellular telephone as claimed by Applicant.

As per claim 72, the type of authorized representative entity disclosed by Ananda is in the form of software. There is no disclosure of providing an authorized representative entity as a hardware device as disclosed and claimed by Applicant.

As per claims 73-74, Ananda does not disclose installing the authorized representative entity on the primary device as claimed. Rather, the authorized representative entity is remotely located at the central rental facility.

As per claim 75, Ananda does not disclose authentication of a secondary device. The authentication steps performed by Ananda with respect to the primary device (user computer) are performed without regard to whether an authorized representative entity is available.

As per claim 76, Ananda discloses that the primary device may terminate the program if the authorization verification passwords do not match. There is no disclosure of controlling access to the software using the secondary device.

As per claim 77, Ananda discloses that the rental security module terminates the application program when the authentication verification passwords do not match. There is no disclosure that the central rental facility (the remote authorized representative entity) controls the access to the software as claimed by Applicant.

As per claim 78, Ananda does not disclose modifying the software so it is unusable to control access to the software. The only access control disclosed by Ananda is terminating execution of the software, not modifying the software as disclosed and claimed by Applicant.

As per claim 79, Ananda discloses transferring the software over a telephone network. There is no disclosure of including the software on a computer readable storage medium as claimed.

As per claim 81, Ananda does not disclose obtaining registration information associated with at least one portable user device. The only registration information obtained by Ananda is the password provided by the user during initial access to the central rental facility, which is not associated with any user device. As such, the

authentication code disclosed by Ananda is not associated with at least one portable device as claimed. In addition, Ananda does not disclose controlling access to the software after transferring the software to a user computer to inhibit access by unauthorized portable user devices as claimed.

As per claim 83, the registration information disclosed by Ananda is provided by the user and therefore is not automatically obtained as claimed by Applicant. In addition, the registration information disclosed by Ananda is not hardware information and is not associated with a portable device as claimed.

As per claim 84, the registration information disclosed by Ananda is not associated with a group of portable devices as claimed.

As per claims 85-87, the authorization verification password disclosed by Ananda is based on the transfer time of the software, the password entered by the user, and the user computer processor clock time. There is no disclosure of providing an authentication code at least partially corresponding to a group of portable devices, a secondary device manufacturer, or a specific type of secondary device as claimed by Applicant.

As per claim 90, Ananda does not disclose a portable user device and therefore does not disclose controlling access to the software using the portable user device.

As per claims 91-92, Ananda does not disclose any portable user devices. The steps of Ananda are performed without regard to whether the software has previously been transferred or installed on the user computer. As such, Ananda does not disclose determining if a portable user device includes an authorized representative entity and transferring the software to the portable user device only if the device includes an authorized representative entity as disclosed and claimed by Applicant.

As per claim 93-95, Ananda discloses terminating execution of the application software if the authorization verification passwords do not match. There is no disclosure of a portable device and no disclosure of modifying the software if the portable device is not authorized to access the software as claimed. In addition, there is no disclosure in Ananda of reducing quality of content contained in the software if the portable device is not authorized (claim 94), and no disclosure of rendering the software unusable on any portable device if the portable device is unauthorized (claim 95).

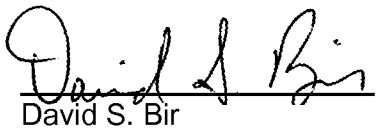
Summary

Applicant's method for securing software as disclosed and claimed in independent claims 1, 40, 48, and 81 includes a number of features that are not disclosed in, and therefore not anticipated by Ananda (US 5,495,411). In addition, numerous features found in the dependent claims are not disclosed by Ananda '411.

Applicants have made a genuine effort to respond to the Examiner's rejections and advance prosecution of this application. Applicants believe that all substantive and formal requirements for patentability have been met and that this case is in condition for allowance, which action is respectfully requested.

No additional fee other than the extension of time fee of $510 and the terminal disclaimer fee of $65 is believed to be due as a result of the filing of this paper. However, please charge any required fees or apply credits to **Deposit Account 50-2841**.

Respectfully submitted:



David S. Bir
Registration No. 38,383

May 20, 2007

Bir Law, PLC
13092 Glasgow Ct.
Plymouth, MI 48170-5241
(734) 927-4531